Appendix II to OMB Circular No. A-130 -

Implementation of the Government Paperwork Elimination Act

AGENCY: Office of Management and Budget, Executive Office of the President

ACTION: Procedures and guidance.

SUMMARY: The Office of Management and Budget (OMB) provides procedures and guidance to implement the Government Paperwork Elimination Act (GPEA). GPEA requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives.

Electronic Availability: This document is available on the Internet in the OMB library of the "Welcome to the White House" home page, http://www.whitehouse.gov/OMB/, the Federal CIO Council's home page, http://cio.gov/, and the Federal Public Key Infrastructure Steering Committee home page, http://gits-sec.treas.gov/.

FOR FURTHER INFORMATION CONTACT: Jonathan Womer, Information Policy and Technology Branch, Office of Information and Regulatory Affairs, (202) 395-3785. Press inquiries should be addressed to the OMB Communications Office, (202) 395-7254. Inquiries may also be addressed to: Information Policy and Technology Branch, Office of Information and Regulatory Affairs, Office of Management and Budget, Room 10236 New Executive Office Building, Washington, D.C. 20503.

SUPPLEMENTARY INFORMATION:

Background

This document provides Executive agencies the guidance required under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII, which was signed into law on October 21, 1998. GPEA is an important tool to improve customer service and governmental efficiency through the use of information technology. This improvement involves transacting business electronically with Federal agencies and widespread use of the

Internet and its World Wide Web.

As public awareness of electronic communications and Internet usage increases, demand for on-line interactions with the Federal agencies also increases. Moving to electronic transactions and electronic signatures can reduce transaction costs for the agency and its partner. Transactions are quicker and information access can be more easily tailored to the specific questions that need to be answered. As a result data analysis is easier. These access and data analysis benefits often have a positive spillover effect into the rest of the agency as awareness of the agency=s operations is improved. In addition, reengineering the work process associated with the transaction around the new electronic format can give rise to other efficiencies.

Public confidence in the security of the government's electronic information processes is essential as agencies make this transition. Electronic commerce, electronic mail, and electronic benefits transfer can require the exchange of sensitive information within government, between the government and private industry or individuals, and among governments. These electronic systems must protect the information's confidentiality, ensure that the information is not altered in an unauthorized way, and make it available when needed. A corresponding policy and management structure must support the hardware and software that delivers these services.

To provide for a broad framework for ensuring the implementation of electronic systems in a secure manner, the Administration has taken a number of actions. In February 1996, OMB revised Appendix III of Circular A-130, which provided guidance to agencies on securing information as they increasingly rely on open and interconnected electronic networks to conduct business. In May 1998, the President issued Presidential Decision Directive 63, which set a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security for government systems by the year 2000 based on reviews by each department and agency. In September, 1998, OMB and the Federal Public Key Infrastructure Steering Committee published AAccess With Trust@ (available at http://gits-sec.treas.gov/). This report describes the Federal government=s goals and efforts to develop a Public Key Infrastructure (PKI) to enable the widespread use of cryptographically-based digital signatures. On December 17, 1999, the President issued a Memorandum, AElectronic Government,@ which called on Federal agencies to use information technology to ensure that governmental services and information are easily accessible to the American people (Weekly Compilation of Presidential Documents, vol. 35, pp. 2641-43, (December 27, 1999); also available at http://cio.gov/). Among other things, the President charged the Administrator of General Services, in coordination with agencies, to assist agencies in the development of private, secure and effective electronic communication across agencies and with the public through the use of public key technology. This technology can offer significant benefits in facilitating electronic commerce through a shared, interoperable, government-wide infrastructure.

What is the purpose of GPEA?

GPEA seeks to Apreclude agencies or courts from systematically treating electronic documents and signatures less favorably than their paper counterparts@, so that citizens can interact with the Federal government electronically (S. Rep. 105-335). It requires Federal agencies, by October 21, 2003, to provide individuals or entities that deal with agencies the option to submit information or transact with the agency electronically, and to maintain records electronically, when practicable. It also addresses the matter of private employers being able to use electronic means to store, and file with Federal agencies, information pertaining to their employees. GPEA states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. It also encourages Federal government use of a range of electronic signature alternatives.

This guidance implements GPEA, fosters a successful transition to electronic government as contemplated by the President=s memorandum, and employs where appropriate the work described in AAccess with Trust.@

What were the comments on the proposed implementation?

On March 5, 1999, OMB published the AProposed Implementation of the Government Paperwork Elimination Act@ for public comment. (64 FR 10896). It was also sent directly to Federal agencies for comment and made available via the Internet. In addition, OMB met with relevant committees and staff of many interested organizations including: American Bar Association (both the Business Law and the Science and Technology Sections); American Bankers Association; National Automated Clearing House Association; National Governors Association; National Association of State Information Resource Executives; National Association of State Auditors, Controllers and Treasurers; National Association of State Purchasing Officers; the Government of Canada; the Government of Australia; and relevant industry forums. All were uniformly positive about the content and tone of the guidance. OMB received specific comments from 24 organizations. Most comments proposed changes in clarity and detail. Where the comments added clarity and did not contradict the goals of the guidance, they were incorporated. The principal substantive issues raised in the comments and our responses to them are described below.

I. Comments regarding risks and benefits

A number of comments, including those from the Justice Department and the General Accounting Office, requested that the guidance contain further information on how to conduct the assessments of practicability needed to determine the proper combination of technology and management controls to manage the risk of converting transactions and record keeping to electronic form, and then conducting transactions electronically. Each assessment should contain elements of risk analysis and measurements of other costs and benefits. Most comments on

assessment referred to the risk analysis portion.

Risk analyses provide decisionmakers with information needed to understand the factors that can degrade or endanger operations and outcomes and to make informed judgments about what actions need to be taken to reduce risk. Consistent with the Computer Security Act (40 U.S.C. 759 note), Appendix III of OMB Circular No. A-130, ASecurity of Federal Automated Information Resources,@ (34 FR 6428, February 20, 1996), Federal managers should design and implement their information technology systems in a manner that is commensurate with the risk and magnitude of harm from unauthorized use, disclosure, or modification of the information in those systems. To determine what constitutes adequate security, a risk-based assessment must consider all major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of current and proposed safeguards. Low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis. OMB reiterated these principles on June 23, 1999, in OMB Memorandum No. 99-20, ASecurity of Federal Automated Information Resources,@ and reminded agencies to continually assess the risk to their computer systems and maintain adequate security commensurate with that risk, particularly as they take increasing advantage of the internet and the world wide web in providing information and services to citizens. (Available at: http://cio.gov/ and http://whitehouse.gov/omb/memoranda/m-99-20.html).

The Commerce Department=s National Institute of Standards and Technology (NIST) also recognizes the importance of conducting risk analyses for securing computer-based resources. NIST provides guidance on risk analysis in (available at http://csrc.nist.gov/nistpubs):

1. AGood Security Practices for Electronic Commerce, Including Electronic Data Interchange,@ Special Publication 800-9 (December 1993);

1. AAn Introduction to Computer Security: The NIST Handbook,@ Special Publication 800-12 (December 1995);

2. AGenerally Accepted Principles and Practices for Securing Information Technology Systems,@ Special Publication 800-14 (September 1996); and

3. AGuide for Developing Security Plans for Information Technology Systems,@ Special Publication 800-18 (December 1998).

More recently, the General Accounting Office published AInformation Security Risk Assessment: Practices of Leading Organizations,@ GAO/AIMD-00-33 (November 1999) (Available at http://www.gao.gov/). This document is intended to help Federal managers implement an ongoing information security risk analysis process by suggesting practical procedures that have been successfully adopted by organizations known for their good risk analysis practices. This document describes various models and methods for analyzing risk, and

identifies factors that are important in a risk analysis.

A quantitative risk analysis generally attempts to estimate the monetary cost of risk compared with that of risk reduction techniques based on (1) the likelihood that a damaging event will occur, (2) the costs of potential losses, and (3) the costs of mitigating actions that could be taken. Availability of data affects the extent to which risk analysis results may be quantified reliably. The GAO report recognizes, however, that reliable data on likelihood and risks often may not be available, in which case a qualitative approach can be taken by defining risk in more subjective and general terms such as high, medium, and low. In this regard, qualitative analyses depend more on the expertise, experience, and good judgment of the Federal managers conducting the analysis. It also may be possible to use a combination of quantitative and qualitative methods.

Other commenters wanted more guidance on how to weigh the risk analysis with other costs and benefits. In combination with the risk analysis, the results of a cost-benefit analysis should be used to judge the practicability of such a process transformation. All major information technology investments are evaluated under the Appendices of OMB Circular No. A-130, AManagement of Federal Information Resources@ and Part 3 of OMB Circular No. A-11 APlanning, Budgeting, and Acquisition of Capital Assets.@ Specific guidance on information technology cost-benefit analysis is available from the Capital Planning and IT Investment Committee of the Federal CIO Council in the recently published AROI and the Value Puzzle.@ (Available at: http://cio.gov/). When developing collections of information under the Paperwork Reduction Act, agencies currently address the practicality of electronic submission, maintenance, and disclosure. The GPEA guidance builds on the requirements and scope of the PRA; all transactions that involve Federal information collections covered under the PRA are also covered under GPEA. In addition, agencies should follow OMB Memorandum 00-07 AIncorporating and Funding Security in Information Systems Investments@, issued February 28, 2000, which provides information on building security into information technology investments (also available at: http://cio.gov/).

The Department of Justice commented on the need for each agency to consider the broad range of legal risks involved in electronic transactions. Justice=s comments are especially appropriate for particularly sensitive transactions, including those likely to give rise to civil or criminal enforcement proceedings and we expect them to be further developed in Juctice=s forthcoming practical guidance. The risk analysis process required by the Computer Security Act and by good practice must be tailored to the risks and related mitigation costs that pertain to each system, as understood by the Federal managers most knowledgeable with the systems. When evaluating legal risks, Federal managers should consult with their legal counsel about any specific legal implications due to the use of electronic transactions or documents in the application in question. Agencies should also keep in mind that GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. We are not, therefore, prescribing specific Aone size fits all@ requirements applicable to transactions regardless of sensitivity.

In light of all the above comments, we have added greater detail to the practicability aspects of

the guidance, and an expanded discussion of cost-benefit analysis and its relation to risk analysis. We have also placed additional emphasis on the need for risk analyses to identify and address the full range of risks, including reasonably expected legal and enforcement risks, and technological risks. Further, we included a reporting mechanism in Part I Section 3 to facilitate the assessment of practicability. Although many of the comments concern the costs and risks of changing to electronic transactions, it is also important to consider the full range of benefits that electronic transactions can provide. Possible benefits include: increased partner participation and customer satisfaction; reduced transaction costs and increased transaction speed; improved record keeping and new opportunities for analysis of information; and greater employee productivity and enhanced quality of their output. An agency-s consideration of risks needs to be balanced with a full consideration of benefits.

II. Comments regarding technology neutrality

A number of comments concerned the emphasis on technology neutrality with regard to the various electronic signature alternatives. They suggested we endorse one electronic signature technology in order to promote interoperability and ease of use. Other commenters disagreed. They expressed concern that promoting one technology requires predicting the direction and future of information technology standards and practices, which is a notoriously difficult task. Further, there are sometimes technologies that naturally fit particular electronic transactions and are easier to implement from a security, privacy, technical, or operational perspective than others. For example, implementing a technology that is easy to use would naturally fit when encouraging citizens to participate in electronic transactions.

We do not believe it would be appropriate to endorse one technology, and we share the concerns of those commenters who argued against such an endorsement. At the same time, we recognize that cryptographically-based digital signatures (i.e., public key technology) hold great promise for ensuring both authentication and privacy in networked interactions, and may be the only technology available that can foster interoperability across numerous applications. There are, however, applications where personal identification numbers (PINs) and other shared secret techniques may well be appropriate. These are generally relatively low risk applications where interoperability is of lesser importance. A number of agencies have successfully used PINs in groundbreaking applications, particularly the Securities and Exchange Commission for regulatory filings and the Internal Revenue Service for tax filings. They have recognized the benefits of using PINs, but at the same time they are planning for an eventual transfer to digital signatures.

Accordingly, the final guidance maintains the basic policy of technology neutrality for automated transactions while recognizing that agencies should select an alternative relative to the risk of the application, and calls on agencies to consider all of the available electronic signature technologies (including the advantages of public key technology) as part of their assessments.

III. Comments regarding records management

Several comments suggested that the guidance should give further emphasis to the role of the National Archives and Records Administration in working with the agencies to address the maintenance, preservation, and disposal of Federal records that are associated with electronic government transactions. We agree. The final guidance explicitly addresses NARA=s role in the area of electronic records management, particularly as it relates to the use of electronic signature technologies.

IV. Comments regarding privacy protection

Some commenters were concerned with the privacy implications of the guidance. They want to ensure that any move to electronic transactions does not encourage the gathering of unnecessary information, and that Federal agencies adequately protect the personal information that does need to be collected. We agree that agencies must incorporate privacy protections when developing electronic processes. Several helpful suggestions were made that have been incorporated into the final guidance. With respect to a commenters= concern that agencies not collect unnecessary information, the Privacy Act requires an agency to Amaintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency.@ 5 U.S.C. 552a(e)(1); see e.g. Reuber v. United States, 829 F. 2d 133, 138-40 (D.C.C. 1987). Furthermore, the collection by agencies of unnecessary information would be contrary to the Paperwork Reduction Act=s mandate that agencies collect only information that is Anecessary for the proper performance of the functions of the agency@ and Ahas practical utility.@ 44 U.S.C. 3508.

V. State, local and non-governmental concerns

A number of comments were received from non-Federal entities. These comments were primarily concerned with the broader implications of the Act itself rather than the draft guidance. Specifically, some governmental entities expressed concern that Federal adoption of routine electronic transactions would require state and local governments to provide equivalent access for citizens. Some commenters were also concerned that they would be required to make all future transactions with the Federal government in an electronic format. Consultations with the state government groups identified above, during and subsequent to the comment period, seem to have alleviated these concerns significantly, particularly as we explained that GPEA contemplates optional rather than mandatory electronic transactions with the Federal government. Agencies are required to provide the option to their transaction partners. Transaction partners are not required to use the electronic option.

What Are the Future Plans for this Guidance?

We intend to place this guidance into an appendix of OMB Circular A-130 as it is updated. OMB=s final procedures and guidance on implementing the Government Paperwork Elimination Act are set forth below.

John T. Spotila*AdministratorOffice of Information and Regulatory Affairs*

April 25, 2000
M-00-10
MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

From: Jacob J. Lew
Director

Subject: OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act

This document provides Executive agencies with the guidance required under Sections 1703 and 1705 the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII. GPEA requires agencies, by October 21, 2003, to provide for the (1) option of electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form.

GPEA is an important tool in fulfilling the vision of improved customer service and governmental efficiency through the use of information technology. This vision contemplates widespread use of the Internet and its World Wide Web, with Federal agencies transacting business electronically as commercial enterprises are doing. Members of the public who wish to do business this way may avoid traveling to government offices, waiting in line, or mailing paper forms. The Federal government can also save time and money transacting business electronically.

This guidance also implements part of the President=s memorandum of December 17, 1999, AElectronic Government,@ which calls on Federal agencies to use information technology in ensuring that governmental services and information are easily accessible to the American people. Among other things, the President charged the Administrator of General Services, in coordination with appropriate agencies and organizations, to assist agencies in developing private, secure, and effective communication across agencies and with the public through the use of digital signature technology.

Creating more accessible and efficient government requires public confidence in the security of the government's electronic information communication and information technology systems. Electronic commerce, electronic mail, and electronic benefits transfer can involve the exchange of sensitive information within government, between government and private industry or individuals, and among governments. Electronic systems must be able to protect the confidentially of citizens= information, authenticate the identity of the transacting parties to the degree required by the transaction, guarantee that the information is not altered in an unauthorized way, and provide access when needed.

To reach these goals, agencies must meet objectives outlined by GPEA guidance. First, each agency must build on their existing efforts to implement electronic government by developing a plan and schedule that implement, by the end of Fiscal Year 2003, optional electronic maintenance, submission, or transactions of information, when practicable as a substitute for paper, including through the use of electronic signatures when practicable. Agencies must submit a copy of the plan to OMB by October 2000 and coordinate the plan and schedule with their strategic IT planning activities that support program responsibilities consistent with the budget process (as required by OMB Circular A-11).

Attachment

Implementation of the Government Paper Work Elimination Act contains:

PART I. What policies and procedures should agencies follow?

PART I. What policies and procedures should agencies follow?

Section 1. What GPEA policies should agencies follow?

The Government Paperwork Elimination Act (GPEA) requires Federal agencies, by October 21, 2003, to provide individuals or entities the option to submit information or transact with the agency electronically and to maintain records electronically when practicable. GPEA specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. It also encourages Federal government use of a range of electronic signature alternatives.

Sections 1703 and 1705 of GPEA charge the Office of Management and Budget (OMB) with developing procedures for Executive agencies to follow in using and accepting electronic documents and signatures, including records required to be maintained under Federal programs and information that employers are required to store and file with Federal agencies about their employees. These procedures reflect and are to be executed with due consideration of the following policies:

a. maintaining compatibility with standards and technology for electronic signatures generally used in commerce and industry and by State governments;

b. not inappropriately favoring one industry or technology;

c. ensuring that electronic signatures are as reliable as appropriate for the purpose in question;

d. maximizing the benefits and minimizing the risks and other costs;

e. protecting the privacy of transaction partners and third parties that have information contained in the transaction;

f. ensuring that agencies comply with their recordkeeping responsibilities under the FRA for these electronic records. Electronic record keeping systems reliably preserve the information submitted, as required by the Federal Records Act and implementing regulations; and

g. providing, wherever appropriate, for the electronic acknowledgment of electronic filings that are successfully submitted.

Section 2. What GPEA procedures should agencies follow?

a. GPEA recognizes that building and deploying electronic systems to complement and

replace paper-based systems should be consistent with the need to ensure that investments in information technology are economically prudent to accomplish the agency's mission, protect privacy, and ensure the security of the data. Moreover, a decision to reject the option of electronic filing or record keeping should demonstrate, in the context of a particular application and upon considering relative costs, risks, and benefits given the level of sensitivity of the process, that there is no reasonably cost-effective combination of technologies and management controls that can be used to operate the transaction and sufficiently minimize the risk of significant harm. Accordingly, agencies should develop and implement plans, supported by an assessment of whether to use and accept documents in electronic form and to engage in electronic transactions. The assessment should weigh costs and benefits and involve an appropriate risk analysis, recognizing that low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis.

b. Performing the assessment to evaluate electronic signature alternatives should not be viewed as an isolated activity or an end in itself. Agencies should draw from and feed into the interrelated requirements of the Paperwork Reduction Act, the Privacy Act, the Computer Security Act, the Government Performance and Results Act, the Clinger-Cohen Act, the Federal Managers' Financial Integrity Act, the Federal Records Act, and the Chief Financial Officers Act, as well as OMB Circular A-130 and Presidential Decision Directive 63.

c. The assessment should develop strategies to mitigate risks and maximize benefits in the context of available technologies, and the relative total costs and effects of implementing those technologies on the program being analyzed. The assessment also should be used to develop baselines and verifiable performance measures that track the agency's mission, strategic plans, and tactical goals, as required by the Clinger-Cohen Act.

d. In addition to serving as a guide for selecting the most appropriate technologies, the assessment of costs and benefits should be designed so that it can be used to generate a business case and verifiable return on investment to support agency decisions regarding overall programmatic direction, investment decisions, and budgetary priorities. In doing so, agencies should consider the effects on the public, its needs, and its readiness to move to an electronic environment.

Section 3. How should agencies implement these policies and procedures?

a. To ensure a smooth and cost-effective transition to an electronic government that provides improved service to the public, each agency must:

(1) Develop a plan (including a schedule) by October, 2000 that provides for continued implementation, by the end of Fiscal Year 2003, of optional electronic maintenance, submission, or transaction of information when practicable as a substitute for paper, including through the use

of electronic signatures when practicable. The plan must address, among other things (and where applicable), the optional use by employers of electronic means to store and file with Federal agencies information about their employees. The plan should prioritize agency implementation of systems or modules of systems based on achievability and net benefit. The plan must be an addition to the agency-s strategic IT planning activities supporting program responsibilities, as required by OMB Circular A-11. A copy of the plan should be provided to OMB.

(2) For each agency information system identified in the plan required in #1 above, consider relative costs, risks, and benefits given the level of sensitivity of the process(es) that the system supports. Agency considerations of cost, risk, and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction. Low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis.

(3) Based on the considerations in #2 each agency in its plan must include:

(a) The name of the information process or group of processes being automated.

(b) A brief description of the information processes being automated. In addition, the description must:

1. Indicate whether further risk management measures are appropriate.

2. Where such measures are appropriate, indicate when and how a combination of information security practices, authentication technologies, management controls, or other business processes for each application will be practicable. In addition, if a particular application is not practicable for conversion to electronic interaction as part of the plan, agencies should explain the reasons and report any strategy to make such conversion practicable.

(c) The date of automation for the information process(es). If the implementation is judged to be not practicable by October 2003, that conclusion may be noted instead of the date. The dates should reflect the prioritization based on achievability and net benefit as discussed in #1 above.

(4) Consistent with the plan take measures (including, if necessary, amending regulations or policies to remove impediments to electronic transactions) to: (a) implement optional electronic submission, maintenance, or disclosure of information and the use of any necessary electronic signature alternatives; and (b) permit private employers who have record keeping responsibilities imposed by the Federal government to store and file information pertaining to their employees electronically.

(5) Ensure that measures taken under the plan reflect appropriate information system confidentiality and security in accordance with the Privacy Act, the Computer Security Act, as amended, and the guidance contained in OMB Circular A-130, Appendices I and III; and ensure that these measures use, to the maximum extent practicable, technologies that are either prescribed in Federal Information Processing Standards promulgated by the Secretary of

Commerce or are supported by voluntary consensus standards as defined in OMB Circular A-119, AFederal Participation in the Development and Use of Voluntary Consensus Standards and Conformity Assessment Activities,@ (63 FR 8546; February 19, 1998).

(6) Report progress annually against the plan (including any appropriate revisions to the schedule) above along with annual performance reporting required under OMB Circular A-11.

(7) Consider the record keeping functionality of any systems that store electronic documents and electronic signatures, to ensure users have appropriate access to the information and can meet the agency=s record keeping needs.

(8) In developing collections of information under the Paperwork Reduction Act, address whether optional electronic submission, maintenance, or disclosure of information (including the electronic storage and filing by employers of information about their employees) would be practicable as a means of decreasing the burden and/or increasing the practical utility of the collection.

b. Department of Commerce

The Department of Commerce must promulgate, in consultation with the agencies and OMB, Federal Information Processing Standards as appropriate to further the specific goals of GPEA. The Department should also develop guidance in the area of authentication technologies and implementations, including cryptographic digital signature technology, with assistance from the Chief Information Officers Council and the Public Key Infrastructure Steering Committee.

c. Department of the Treasury

The Department of the Treasury must develop, in consultation with the agencies and OMB, policies and practices for the use of electronic transactions and authentication techniques for use in Federal payments and collections and ensure that they fulfill the goals of GPEA.

d. Department of Justice

The Department of Justice must develop, in consultation with the agencies and OMB, practical guidance on legal considerations related to agency use of electronic filing and record keeping.

e. National Archives and Records Administration

The National Archives and Records Administration must develop, in consultation with the agencies and OMB, policies and guidance on the management, preservation, and disposal of Federal records associated with electronic government transactions, and must give particular consideration to records issues associated with the use of electronic signature technologies.

f. General Services Administration

The General Services Administration must support agencies' implementation of digital signature technology and related electronic service delivery.

g. Office of Management and Budget

OMB must provide continuing guidance and oversight for the implementation of GPEA, including through its review of collections of information under the Paperwork Reduction Act.

Part II. How can agencies improve service delivery and reduce burden through the use of electronic signatures and electronic transactions?

This part provides Federal managers with basic information to assist in planning for an orderly and efficient transition to electronic government. Agencies should begin their planning promptly to ensure compliance with the timetable in GPEA.

Section 1. Introduction and background.

a. As required by GPEA, this Part provides guidance to agencies for deciding whether to use electronic signature technology for a particular application. GPEA requires Federal agencies, by October 21, 2003, to allow individuals or entities the option to submit information or transact with the agencies electronically and to maintain records electronically, when practicable. It specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form. It also encourages Federal government use of a range of electronic signature alternatives. The guidance helps agencies consider which electronic signature technology may be most appropriate and suggests methods to maximize the benefit of electronic information while minimizing risk when implementing a particular electronic signature technology to secure electronic transactions.

The guidance builds on the requirements and scope of the Paperwork Reduction Act of 1995 (PRA). According to the PRA agencies must, "consistent with the Computer Security Act of 1987 (CSA) (40 U.S.C. 759 note), identify and afford security protections commensurate with

the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency." 44 U.S.C. 3506(g)(3). In addition, we note that all transactions that involve Federal information collections covered under the PRA are also covered under GPEA.

b. As GPEA, PRA, CSA, and the Privacy Act recognize, the goal of information security is to protect the integrity and confidentiality of electronic records and transactions that enable business operations. Different security approaches offer varying levels of assurance in an electronic environment and are appropriate depending on a balance between the benefits from electronic information transfer and the risk of harm if the information is compromised. Among these approaches (in an ascending level of assurance) are:

(1) so-called "shared secrets" methods (e.g., personal identification numbers or passwords),

(2) digitized signatures or biometric means of identification, such as fingerprints, retinal patterns, and voice recognition, and

(3) cryptographic digital signatures (discussed in more detail in Section 7).

Combinations of approaches (e.g., digital signatures with biometrics) are also possible and may provide even higher levels of assurance than single approaches by themselves. Deciding which to use in an application depends first upon finding a balance between the risks associated with the loss, misuse, or compromise of the information, and the benefits, costs, and effort associated with deploying and managing the increasingly secure methods to mitigate those risks. Agencies must strike a balance, recognizing that achieving absolute security is likely to be highly improbable in most cases and prohibitively expensive if possible.

Section 2. What is an "electronic signature?"

a. GPEA defines "electronic signature" as follows:

A . . . a method of signing an electronic message that --

(A) identifies and authenticates a particular person as the source of the electronic message; and

(B) indicates such person's approval of the information contained in the electronic message.@ (GPEA, section 1709(1)).

This definition is consistent with other accepted legal definitions of signature. The term "signature" has long been understood as including "any symbol executed or adopted by a party with present intention to authenticate a writing." (Uniform Commercial Code, 1-201(39)(1970)). The AUniform Electronic Transactions Act,@ recently adopted by the National Conference of Commissioners of Uniform State Laws, and which is being enacted by the States, contains a

similar definition (see http://www.nccusl.org). These flexible definitions permit the use of different electronic signature technologies, such as digital signatures, personal identifying numbers, and biometrics (section 7 provides more detail on electronic signature technologies). While it is the case that, for historical reasons, the Federal Rules of Evidence are tailored to support the admissibility of paper-based evidence, the Federal Rules of Evidence have no actual bias against electronic evidence.

b. In enacting GPEA, Congress addressed the legal effect and validity of electronic signatures or other electronic authentication:

AElectronic records submitted or maintained in accordance with procedures developed under this title, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, must not be denied legal effect, validity, or enforceability because such records are in electronic form@ (GPEA, section 1707).

Section 3. How should agencies assess the risks, costs, and benefits?

To evaluate the suitability of electronic signature alternatives for a particular application, the agency needs to perform an assessment. The assessment should include a risk analysis, in cases where the sensitivity of the transaction is sufficiently great, and a cost-benefit analysis. The assessment identifies the particular technologies and management controls best suited to minimizing the risk and cost to acceptable levels, while maximizing the benefits to the parties involved. Often parts of the assessment can be quantified, but some factors - particularly the risk analysis B usually can only be estimated qualitatively.

Availability of data affects the extent to which risk can be reliably quantified. A quantitative approach to risk analysis generally attempts to estimate the monetary cost of risk compared to the cost of risk reduction techniques based on:

(i) the likelihood that a damaging event will occur,

(ii) the costs of potential losses, and

(iii) the costs of mitigating actions that could be taken.

Reliable data on likelihood and costs may not be available. In this case a qualitative approach can be taken by defining risk in more subjective and general terms such as high, medium, and low. In this regard, qualitative analyses depend more on the expertise, experience, and good judgment of the Federal managers conducting them than on quantified factors.

The same can be true with other costs and benefits. Some factors, such as the value of deterring fraud, are difficult to quantify. If a new automated system is less secure than an old, paper-based system, attempts to commit fraud or to repudiate transactions may increase. It

usually is not possible to quantify in monetary terms attitudes such as increased customer satisfaction and willingness to cooperate with an agency, which may result from electronic processes designed to be user-friendly. However, many costs (design, development, and implementation) and benefits (reduced transaction costs, saved time etc.) can be quantified, as is the case for other IT projects. Clearly, then, the assessment should use a combination of quantitative and qualitative methods to judge the practicability of any electronic transaction method and should include a comprehensive risk analysis when warranted by the sensitivity of the data and/or the transaction.

Those alternatives that minimize risk to an acceptable level should be assessed in terms of net benefit to the agency and the customer in order to determine the electronic signature most appropriate for the transaction. If the net benefits are negative, the agency may determine that using an electronic process is not practicable at this time. In any event, all risk analyses are exercises in managerial judgment.

a. Consider the costs of risk mitigation. The assessment must recognize that neither handwritten signatures nor electronic signatures are totally reliable and secure. Every method of signature, whether electronic or on paper, can be compromised with enough skill and resources, or due to poor security procedures, practices, or implementation. Setting up a very secure, but expensive, automated system may in fact buy only a marginal benefit of deterrence or risk reduction over other alternatives and may not be worth the extra cost. For example, past experience with fraud risks, and a careful analysis of those risks, shows that exposure is often low. If this is the case a less expensive system that substantially deters fraud is warranted, and not an absolutely secure system. Overall, security determination should conform to the Computer Security Act: the level of security should be commensurate with the level of sensitivity of the transaction.

b. Conduct a cost-benefit analysis to determine if an electronic transaction is practicable. The primary goal of a cost-benefit analysis should be to find a cost-effective package of security mechanisms and management controls that can support automated systems using electronic communications. In estimating the cost of any system, agencies should include costs associated with hardware, software, administration, and support of the system, both short-term and long-term. Agencies should consider the following issues when framing the cost-benefit analysis:

(1) Offering more than one way to communicate electronically may enable more people to conduct electronic transactions. If different partners have different skills and differing security concerns, providing a combination of mechanisms will meet the needs of a greater number of possible partners. While admittedly adding cost, offering multiple alternatives can add greater benefit, as well. Under GPEA, the agency must considered this option whenever it expects to receive over 50,000 electronic submittals (per year) of a particular form.

(2) Electronic transactions can impose costs on the transaction partners. Many electronic signature techniques require specialized computer hardware and technical knowledge. The higher these threshold costs are, the higher the participation costs are for users. Higher costs will tend to narrow the range of potential users, which in turn limits the benefits of electronic communications.

(3) Agencies should assess the costs of developing and maintaining electronic transactions. Information technology costs continue to fall and electronic signature techniques continue to evolve. As a result, the agency should periodically redo its risk and cost-benefit analyses on those programs where electronic transactions were initially deemed impracticable to determine whether costs and/or technologies have changed enough so that electronic transactions have become practicable.

(4) If the cost-benefit analysis of a proposed solution indicates that the electronic solution is not cost effective, the agency should seek to identify opportunities to reengineer the underlying process being automated. Occasionally, practices and rules under the control of an agency are based on factors or circumstances that may no longer apply. In these cases new practices and rules should be proposed if the changes do not undermine the objective or impair security, and if the changes lead to a more efficient process.

c. Document the decision. The Computer Security Act gives agency managers the responsibility to select an appropriate combination of technologies, practices, and management controls to minimize risk cost-effectively while maximizing benefits to all parties to the transaction. Agency managers should document these decisions, however qualitative, in the system security plan (see the NIST AGuide for Developing Security Plans for Information Technology Systems,@ Special Publication 800-18 (December 1998)) for later review and adjustment.

Section 4. What benefits should agencies consider in planning and implementing electronic signatures and electronic transactions?

Benefits from moving to electronic transactions and electronic signatures include reduction in transaction costs for the agency and the transaction partner. Transactions are quicker and it is often easier to access information related to the transaction because it is in electronic form. The electronic form often allows more effective data analysis because the information is easier to access. Better data analysis often improves the operation of the newly electronic transaction. In addition, if many transactions are electronic and data analysis can be done across transactions the benefits can spillover into the rest of the agency as operational awareness of the entire organization is improved. Moreover, business process reengineering should accompany all attempts to facilitate a transaction through information technology. Often the full benefits will be realized only by restructuring the process to take advantage of the technology. Merely moving an existing paper based process to an electronic one is unlikely to reap the maximum benefits from

the electronic system.

In order to account for all the benefits associated with electronic transactions, agencies should keep common information technology benefits in mind and look at the benefits realized by other agencies.

a. What are the benefits? Agencies should identify all the benefits of automating program transactions and making those transactions secure, such as:

(1) Increased speed of the transaction. The partner and the agency may spend less time completing the transaction. The quicker speed combined with putting the transaction online allows real-time help to the transaction partner, providing a benefit not found in a paper based transaction.

(2) Increased partner participation and customer satisfaction. Often a decrease in partner transaction costs leads to more partners completing the transaction. In addition, partners tend to have a more positive view of the process given its speed and ease of use.

(3) Improved record keeping efficiency and data analysis opportunities. If data are easier to access and store then they can enhance program evaluation and expand awareness of the effects of the government program in question.

(4) Increased employee productivity and improved quality of the final product. Electronic transactions tend to have fewer errors because often the system minimizes retyping and automatically detects certain errors. These benefits allow the employees to concentrate more time on other matters.

(5) Greater information benefits to the public. Moving to electronic transactions and electronic signatures often can make the related information more accessible to the public and Freedom of Information Act requests.

(6) Improved security. Designed, implemented, and managed properly, electronic transactions can have fewer opportunities for fraud and more robust security measures than paper and envelope transactions.

(7) Extensive security for highly sensitive information. Even though implementing a more secure electronic signature option often is more expensive initially than implementing less secure alternatives, there could be larger expected benefits if the information being protected is particularly sensitive.

b. What are examples of benefits from electronic signatures and transactions? The following examples highlight agencies= experience in gaining significant benefits from electronic transactions and electronic signatures.

(1) The Internal Revenue Service uses electronic identification to strengthen validation by incorporating electronic links between the user and preexisting data about that user in the agency's records in its TeleFile program. It enables selected taxpayers to file 1040EZs with a touch-tone phone. Taxpayers get Customer Service Numbers (CSNs, i.e., PINs) that they then use to sign their returns and which help to validate their identities to the agency. Even though a CSN is not unique to an individual taxpayer (since it is only five digits long), the IRS authenticates the filer by using other identifying factors, such as the taxpayer's date of birth, taxpayer identification number, and by using additional procedures. This approach is not used over the Internet. Instead, it occurs in short-term connections over telephone lines, an environment where it is comparatively difficult for persons to eavesdrop and steal information or substitute false information.

(2) Taxpayers who transmit their tax returns electronically give high marks to the Internal Revenue Service=s electronic filing programs. The American Customer Satisfaction Index (ACSI) shows customer satisfaction scores for IRS e-file exceed those for both the government and retail sectors and rival those of the financial services sector. For electronic tax return filers, the overall ACSI customer satisfaction index is 74. This surpasses the rating among paper return filers and compares with a government-wide satisfaction rating of 68.6. In addition, 78% of customers with electronic filing experiences say they are more satisfied now than two years ago. Other benefits of the electronic filing program include:

(a) Refunds are received in half the time and even faster with Direct Deposit.

(b) Its accuracy rate of over 99% reduces the chance of getting an error notice from the IRS.

(c) It provides an IRS acknowledgment within 48 hours that the return has been received.

(3) The General Services Administration, Federal Technology Service conducted the FTS2001 Procurement in a totally paperless environment. Beginning with the Request for Proposals (RFP) release, which was digitally signed and posted on the internet along with a utility for verifying the signature, through the issuance of the contracts to the winning bidders in an electronic signing ceremony, no paper changed hands at any time during the process. Bids from the offerors were delivered on a single CD, in contrast with the previous FTS2000 solicitation that required several pallets of documentation for each submission. It is estimated that the paper equivalent of this bid would have resulted in a stack of paper approximately 5 stories high. This electronic process resulted in efficiencies and savings to the government of approximately $1,500,000 in time previously required to process paperwork. The paperless process was enabled by issuing each potential bidder a cryptographically-based digital signature certificate housed on a hardware token.

(4) EDGAR, the Electronic Data Gathering, Analysis, and Retrieval system, performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required by law to file forms with the U.S. Securities and Exchange Commission (SEC). Its primary purpose is to increase the efficiency and fairness of the

securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency. Other benefits include:

(a) Elimination of the burdens and delays associated with microfiching 10-12 million pages of information annually in a paper format.

(b) Free SEC web site experiences over half a million hits daily, many from individuals trying to improve the quality of their investment decisions by examining disclosure documents. Prior to EDGAR, individuals simply could not afford the typical, minimum cost of $25 per document.

(c) Full search capability allows improved ability to identify incidents of new or unusual conditions in the reports that are filed and allow rapid access to the information.

(5) The U.S. Customs Service automated much of the information transactions with its import-export partners. It has allowed improved accuracy, efficiency, speed, and the ability to analyze the electronically filed data which has led to enforcement improvements. The Automated Commercial System (ACS) is the system used to track, control, and process all commercial goods imported into the United States. ACS facilitates merchandise processing, significantly cuts costs, and reduces paperwork requirements for both Customs and the trade community.

Section 5. What risk factors should agencies consider in planning and implementing electronic signatures or electronic transactions?

Properly implemented electronic signature technologies can offer degrees of confidence in authenticating identity that are greater than a handwritten signature can offer. These digital tools should be used to control risks in a cost-effective manner. In determining whether an electronic signature is sufficiently reliable for a particular purpose, agency risk analyses need at a minimum to consider the relationships between the parties, the value of the transaction, the risk of intrusion, and the likely need for accessible, persuasive information regarding the transaction at some later date. In addition, agencies should consider any other risks relevant to the particular process. Once these factors are considered separately, an agency should consider them together to evaluate the sensitivity to risk of a particular process, relative to the benefit that the process can bring.

a. What is the relationship between the parties? Agency transactions fall into seven general categories, each of which may be vulnerable to differing security risks:

(1) Intra-agency transactions (i.e., those which remain within the same Federal agency).

(2) Inter-agency transactions (i.e., those between Federal agencies).

(3) Transactions between a Federal agency and state or local government agencies.

(4) Transactions between a Federal agency and a private organization such as: contractor, business, university, non-profit organization, or other entity.

(5) Transactions between a Federal agency and a member of the general public.

(6) Transactions between a Federal agency and a foreign government, foreign private organization, or foreign citizen.

Risks tend to be relatively low in cases where there is an ongoing relationship between the parties. Generally speaking, there will be little risk of a partner later repudiating inter- or intra-governmental transactions of a relatively routine nature, and almost no risk of the governmental trading partner committing fraud. Similarly, transactions between a regulatory agency and a publicly traded corporation or other known entity regulated by that agency can often bear a relatively low risk of repudiation or fraud, particularly where the regulatory agency has an ongoing relationship with, and enforcement authority over, the entity. For the same reasons, risks tend to be relatively low within rulemaking contexts, as all parties can view the submissions of others so the risk of imposture is minimized. Other types of transactions, involving an ongoing relationship between an agency and non-governmental entities and persons, can have varying degrees of risk depending on the nature of the relationship between the parties; the same would apply in the case of those Federal programs in which the ongoing relationship is between entities that are acting (and collecting information under the PRA) on behalf of an agency and such non-governmental entities and persons -- e.g., transactions between a lender, guaranty agency, or other institution participating in a Federal loan or financial aid program and another program participant or a member of the general public, such as a borrower or grant recipient. On the other hand, the highest risk of fraud or repudiation is for a one-time transaction between a person and an agency that has legal or financial implications. Agencies should also pay attention to transactions with non-Federal entities, where the agency has a law enforcement responsibility but does not have an ongoing relationship. Transactions between a Federal agency and a foreign entity may entail unique legal risks due to varying national laws and regulations. In all cases, the relative value of the transaction needs to be considered as well.

b. What is the value of the transaction? Agency transactions fall into five general categories, each of which may be vulnerable to different security risks:

(1) Transactions involving the transfer of funds.

(2) Transactions where the parties commit to actions or contracts that may give rise to financial or legal liability.

(3) Transactions involving information protected under the Privacy Act or other agency-specific statutes, or information with national security sensitivity, obliging that access to the information be restricted.

(4) Transactions where the party is fulfilling a legal responsibility which, if not performed, creates a legal liability (criminal or civil).

(5) Transactions where no funds are transferred, no financial or legal liability is involved and no privacy or confidentiality issues are implicated.

Agency risk analyses should attempt to identify the relative value of the type of transaction being automated and factor that against the costs associated with implementing technological and management controls to mitigate risk. Note that the value of the transaction depends on the perspective of the agency and the transaction partner. In general, electronic signatures are least necessary in very low value transactions and need not be used unless specifically required by law or regulation (i.e. #5). Where authentication is necessary, the method of electronic signature should be appropriate to the level of risk.

c. What is the risk of intrusion? The probability of a security intrusion on the transaction can depend on the benefit to the potential attackers and their knowledge that the transaction will take place. Agency transactions fall into three categories:

(1) Regular or periodic transactions between parties are at a higher risk than intermittent transactions because of their predictability, causing higher likelihood that an outside party would know of the scheduled transaction and be prepared to intrude on it.

(2) The value of the information to outside parties could also determine their motivation to compromise the information. Information relatively unimportant to an agency may have high value to an outside party.

(3) Certain agencies, because of their perceived image or mission, may be more likely to be attacked independent of the information or transaction. The act of disruption can be an end in itself.

d. What is the likely need for accessible, persuasive information regarding the transaction at a later point? Agency transactions fall into seven general categories:

(1) Transactions where the information generated will be used for a short time and discarded;

(2) Transactions where the information generated may later be subject to audit or compliance;

(3) Transactions where the information will be used for research, program evaluation, or other statistical analyses;

(4) Transactions where the information generated may later be subject to dispute by one of the parties (or alleged parties) to the transaction;

(5) Transactions where the information generated may later be subject to dispute by a non-party to the transaction;

(6) Transactions where the information generated may later be needed as proof in court;

(7) Transactions where the information generated will be archived later as permanently valuable records.

When analyzing the benefits of converting from paper systems to electronic systems, agencies should reflect on what information would be lost in the conversion, e.g., an envelope containing a postmark and the sender's fingerprints and handwriting, or the specific questions that were asked on a questionnaire. Agencies should determine whether collecting the potentially lost information is truly important and whether an electronic system could cost-effectively collect and store similarly useful information.

In some paper transactions requiring a party's signature, the signature both identifies the party and establishes that party's intent to submit a truthful answer. Sometimes a notary or other third party signs as witness to the signature. When converting these transactions to electronic systems, agencies should ensure that the selected technology and its implementation are able to provide similar functions.

Section 6. What privacy and disclosure issues affect electronic signatures and electronic transactions?

Section 1708 of GPEA limits the use of information collected in electronic signature services to communications with a Federal agency. It directs agencies and their staff and contractors not to use such information for any purpose other than for facilitating the communication. Exceptions exist if the person (or entity) that is the subject of the information provides affirmative consent to the additional use of the information, or if such additional use is otherwise provided by law. Accordingly, agencies should follow several privacy principles:

a. Electronic signatures should only be required where needed. Many transactions do not need, and should not require, identifying or other information about an individual. For example, individuals generally should not be required to provide personal information in order to download public documents.

b. When electronic signatures are required for a transaction, agencies should not collect more information from the user than is required for the application of the electronic signature. When appropriate, agencies are encouraged to use methods of electronic signing that do not require individuals to disclose their identity. This includes the ability of individuals in a group to be identified by a group identifier rather than an individual identifier if the only information needed to authenticate is the fact that that the individual is a member of the group.

c. Users should be able to decide how, when, and what type of electronic authentication to use of those made available by the agency. If none are acceptable the user should be able to opt out to a paper process. If a user wants a certain mechanism for authentication to apply only to a single agency or to a single type of transaction, the user's desires should be honored, if practicable. Conversely, if the user wishes the authentication to work with multiple agencies or for multiple types of transactions, that should also be permitted where practicable. Specifically, it should be consistent with how the agency employs such means of authentication and with relevant statute and regulation and only if it conforms to practicable costs and risks.

d. Agencies should ensure, and users should be informed, that information collected for the purpose of issuing or using electronic means of authentication will be managed and protected in accordance with applicable requirements under the Privacy Act, the Computer Security Act, and any agency-specific statute mandating the protection of such information, as well as with any relevant Executive Branch and agency specific privacy policies.

Section 7. What are current electronic signature technologies?

Questions regarding the following should be directed to the Department of Commerce. This section addresses two categories of security: 1) Non-cryptographic methods of authenticating identity; and 2) cryptographic control methods. The non-cryptographic approach relies solely on an identification and authentication mechanism that must be linked to a specific software platform for each application. Cryptographic controls may be used for multiple applications, if properly managed, and may encompass both authentication and encryption services. A highly secure implementation may combine both categories of technologies. The spectrum of electronic signature technologies currently available is described below.

a. Non-Cryptographic Methods of Authenticating Identity

(1) Personal Identification Number (PIN) or password: A user accessing an agency's electronic application is requested to enter a "shared secret" (called "shared" because it is known both to the user and to the system), such as a password or PIN. When the user of a system enters her name, she also enters a password or PIN. The system checks that password or PIN against data in a database to ensure its correctness and thereby "authenticates" the user. If the authentication process is performed over an open network such as the Internet, it is usually essential that at least the shared secret be encrypted. This task can be accomplished by using a technology called Secure Sockets Layer (SSL), which uses a combination of public key technology and symmetric cryptography to automatically encrypt information as it is sent over the Internet by the user and decrypt it before it is read by the intended recipient. SSL currently is built into almost all popular Web browsers, in such a fashion that its use is transparent to the end user. Assuming the password is protected during transmission, as described above, impersonating the user requires obtaining the user-s password. This may be relatively easy if users do not follow appropriate guidelines for password creation and use. Agencies should establish adequate guidelines for

password creation and protection.

(2) Smart Card: A smart card is a plastic card the size of a credit card containing an embedded integrated circuit or Achip@ that can generate, store, and/or process data. It can be used to facilitate various authentication technologies also embedded on the same card. By having different authentication choices the user can pick the authentication technique that meets but does not exceed the information requirement for the transaction. A user inserts the smart card into a card reader device attached to a computer or network input device. Information from the card's chip is provided to the computer only when the user also enters a PIN, password, or biometric identifier recognized by the card. Thus, the user authenticates to the card, making available electronic credentials which can then be used by the computer or network to strongly authenticate the user for transactions. This method offers far greater security than the typical use of a PIN or password, because the shared secret is between the user and the card, not with a remote server or network device. Moreover, to impersonate the user requires possession of the card as well as knowledge of the shared secret that activates the electronic credentials on the card. Thus, proper security requires that the card and the PIN or password used to activate it be kept separate. This is not a concern if a biometric is used for the latter purpose.

(3) Digitized Signature: A digitized signature is a graphical image of a handwritten signature. Some applications require an individual to create his or her hand-written signature using a special computer input device, such as a digital pen and pad. The digitized representation of the entered signature may then be compared to a previously-stored copy of a digitized image of the handwritten signature. If special software judges both images comparable, the signature is considered valid. This application of technology shares the same security issues as those using the PIN or password approach, because the digitized signature is another form of shared secret known both to the user and to the system. The digitized signature can be more reliable for authentication than a password or PIN because there is a biometric component to the creation of the image of the handwritten signature. Forging a digitized signature can be more difficult than forging a paper signature since the technology digitally compares the submitted signature image with the known signature image, and is better than the human eye at making such comparisons. The biometric elements of a digitized signature, which help make it unique, are in measuring how each stroke is made B duration, pen pressure, etc. As with all shared secret techniques, compromise of a digitized signature image or characteristics file could pose a security (impersonation) risk to users.

(4) Biometrics: Individuals have unique physical characteristics that can be converted into digital form and then interpreted by a computer. Among these are voice patterns (where an individual's spoken words are converted into a special electronic representation), fingerprints, and the blood vessel patterns present on the retina (or rear) of one or both eyes. In this technology, the physical characteristic is measured (by a microphone, optical reader, or some other device), converted into digital form, and then compared with a copy of that characteristic stored in the computer and authenticated beforehand as belonging to a particular person. If the test pattern and the previously stored patterns are sufficiently close (to a degree which is usually selectable by the authenticating application), the authentication will be accepted by the software,

and the transaction allowed to proceed. Biometric applications can provide very high levels of authentication especially when the identifier is obtained in the presence of a third party to verify its authenticity, but as with any shared secret, if the digital form is compromised, impersonation becomes a serious risk. Thus, just like PINs, such information should not be sent over open networks unless it is encrypted. Moreover, measurement and recording of a physical characteristic could raise privacy concerns where the biometric identification data is shared by two or more entities. Further, if compromised, substituting a different, new biometric identifier may have limitations (e.g., you may need to employ the fingerprint of a different finger). Biometric authentication is best suited for access to devices, e.g. to access a computer hard drive or smart card, and less suited for authentication to software systems over open networks.

b. Cryptographic Control

Creating electronic signatures may involve the use of cryptography in two ways: symmetric (or shared private key) cryptography, or asymmetric (public key/private key) cryptography. The latter is used in producing digital signatures, discussed further below.

(1) Shared Symmetric Key Cryptography

In shared symmetric key approaches, the user signs a document and verifies the signature using a single key (consisting of a long string of zeros and ones) that is not publicly known, or is secret. Since the same key does these two functions, it must be transferred from the signer to the recipient of the message. This situation can undermine confidence in the authentication of the user's identity because the symmetric key is shared between sender and recipient and therefore is no longer unique to one person. Since the symmetric key is shared between the sender and possibly many recipients, it is not private to the sender and hence has lesser value as an authentication mechanism. This approach offers no additional cryptographic strength over digital signatures (see below). Further, digital signatures avoid the need for the shared secret.

(2) Public/Private Key (Asymmetric) Cryptography - Digital Signatures

(a) To produce a digital signature, a user has his or her computer generate two mathematically linked keys -- a private signing key that is kept private, and a public validation key that is available to the public. The private key cannot be deduced from the public key. In practice, the public key is made part of a "digital certificate," which is a specialized electronic file digitally signed by the issuer of the certificate, binding the identity of the individual to his or her private key in an unalterable fashion. The whole system that implements digital signatures and allows them to be used with specific programs to offer secure communications is called a Public Key Infrastructure, or PKI.

(b) A "digital signature" is created when the owner of a private signing key uses that key to

create a unique mark (the signature) on an electronic document or file. The recipient employs the owner's public key to validate that the signature was generated with the associated private key. This process also verifies that the document was not altered. Since the public and private keys are mathematically linked, the pair is unique: only the public key can validate signatures made using the corresponding private key. If the private key has been properly protected from compromise or loss, the signature is unique to the individual who owns it, that is, the owner cannot repudiate the signature. In relatively high-risk transactions, there is always a concern that the user will claim some else made the transaction. With public key technology, this concern can be mitigated. To claim he did not make the transaction, the user would have to feign loss of the private key. By creating and holding the private key on a smart card or an equivalent device, and by using a biometric mechanism (rather than a PIN or password) as the shared secret between the user and the smart card for unlocking the private key to create a signature this concern can be mitigated. In other words, combining two or three distinct electronic signature technology approaches in a single implementation can enhance the security of the interaction and lower the potential for fraud to almost zero. Furthermore, by establishing clear procedures for a particular implementation of digital signature technology, so that all parties know what the obligations, risks, and consequences are, agencies can also strengthen the effectiveness of a digital signature solution.

The reliability of the digital signature is directly proportional to the degree of confidence one has in the link between the owner's identity and the digital certificate, how well the owner has protected the private key from compromise or loss, and the cryptographic strength of the methodology used to generate the public-private key pair. The cryptographic strength is affected by key length and by the characteristics of the algorithm used to encrypt the information. Further information on digital signatures can be found in AAccess with Trust@ (September 1998) (**http://gits-sec.treas.gov/).**

c. Technical Considerations of the Various Electronic Signature Alternatives

(1) To be effective, each of these methods requires agencies to develop a series of policy documents that provide the important underlying framework of trust for electronic transactions and which facilitate the evaluation of risk. The framework identifies how well the user=s identity is bound to his authenticator (e.g., his password, fingerprint, or private key). By considering the strength of this binding, the strength of the mechanism itself, and the sensitivity of the transaction, an agency can determine if the level of risk is acceptable. If an agency has experience with the technology, existing policies and documents may be available for use as guidance. Where the technology is new to an agency, this may require additional effort.

(2) While digital signatures (i.e. public key/private key) are generally the most certain method for assuring identity electronically, the policy documents must be established carefully to achieve the desired strength of binding. The framework must identify how well the signer's identity is bound to his or her public key in a digital certificate (identity proofing). The strength of this

binding depends on the assumption that only the owner has sole possession of the unique private key used to make signatures that are validated with the public key. The strength of this binding also reflects whether the private key is placed on a highly secure hardware token, such as a smart card, or is encapsulated in software only; and how difficult it is for a malefactor to deduce the private key using cryptographic methods (which depends upon the key length and the cryptographic strength of the key-generating algorithm).

A Public Key Infrastructure (PKI) is one mechanism to support the binding of public keys with the user=s identity. A PKI can provide the entire policy and technical framework for the systematic and diligent issuance, management and revocation of digital certificates, so that users who wish to rely on someone=s certificate have a firm basis to check that the certificate has not been maliciously altered, and to confirm that it remains active (i.e., has not been revoked because of loss or compromise of the corresponding private key). This same infrastructure provides the basis for interoperability among different agencies or entities, so that a person=s digital certificate can be accepted for transactions by organizations external to the one that issued it.

(3) By themselves, digitized (not digital) signatures, PINs, biometric identifiers, and other shared secrets do not directly bind identity to the contents of a document as do digital signatures which actually use the document information to make the signature. For shared secrets to bind the user=s identity to the document, they must be used in conjunction with some other mechanism. Biometric identifiers such as retinal patterns used in conjunction with digital signatures can offer far greater proof of identify than pen and ink signatures.

(4) While not as robust as biometric identifiers and digital signatures, PINs have the decided advantage of proven customer and citizen acceptance, as evidenced by the universal use of PINs for automated teller machine transactions. PINs combined with encrypted Internet sessions, particularly through the use of Secure Sockets Layer technology on the World Wide Web, are very popular for retail consumer transactions requiring credit card or other personal authenticating information. This may well be suited for a variety of government applications. Also, secure Web browsers are increasingly being designed to accommodate digital signatures, making this approach a possible interim step towards implementing the more robust authentication provided by digital signatures.

(5) It is important to remember that technical factors are but one aspect to be considered when an agency plans to implement electronic signature-based applications. Other important aspects are considered in the following sections.

Section 8. How should agencies implement electronic signatures and electronic transactions?

After the agency has conducted the assessment and identified an appropriate electronic signature technology alternative that may be used to secure an automated business process, the agency will proceed to implement this decision. For any electronic transaction, agencies should collect and record adequate information regarding the content, process, and identities of the parties involved.

In doing so, agencies should consider the following:

a. Build from a policy framework. GPEA applies to interactions between outside entities and the Federal government, as well as to transactions and record keeping required by parties under Federal programs. Accordingly, agencies should consider whether their policies or programmatic regulations support the use and enforceability of electronic signature alternatives to handwritten signatures as well as to electronic record keeping under Federal programs. If necessary, agencies should develop a strategy to make any revisions needed to achieve this goal. In addition, by clearly informing the transaction partners that electronic signatures and records will be acceptable and used for enforcement purposes, their legal standing is enhanced. Several agencies have already chosen to promulgate policies or regulations on this issue, including:

1) Securities and Exchange Commission (17 C.F.R. Part 232), electronic regulatory filings;

2) Environmental Protection Agency (55 Fed. Reg. 31,030 (1990)), policy on electronic reporting;

3) Food and Drug Administration (21 C.F.R. Part 11), electronic signatures and records;

4) Internal Revenue Service (Treasury Reg. 301.6061-1), signature alternatives for tax filings;

5) Federal Acquisition Regulation (48 C.F.R. Parts 2 and 4), electronic contracts;

6) General Services Acquisition Regulation (48 C.F.R. Part 552.216-73), electronic orders;

7) Federal Property Management Regulations (41 C.F.R. Part 101-41), electronic bills of lading.

8) Administrative Committee of the Federal Register (1 C.F.R. Part 18.7), electronic signatures on documents submitted for publication in the *Federal Register*.

9) Commodity Futures Trading Commission (17 C.F.R. Part 1.4 and Part 1.3(tt)), electronic signatures for filings.

When specifying the requirements for electronic record keeping by regulated entities or government business partners (e.g. contractors or grantees), particularly the maintenance of electronic forms pertaining to employees by employers, agencies should consult the "Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems," developed by the Association for Information and Image Management (ANSI/AIIM TR31). This set of documents offers suggestions for maximizing the likelihood that electronically filed and stored records will be accorded full legal recognition. If an agency chooses to use digital signature technology, a regulation might specify that each individual will be issued a unique digital signature certificate to use, agree to keep the private key confidential, agree to accept responsibility for anything that is submitted using that key, or accept other conditions under which the agency will accept electronic submissions.

b. Where necessary, use a mutually understood, signed agreement between the person or entity submitting the electronically-signed information and the receiving Federal agency.

As a matter of efficiency, arrangements with large numbers of customers may be best accomplished by setting forth an agency's terms and conditions in a policy or regulation. Arrangements with smaller numbers of customers may lend themselves to one or more agreements, using a document referred to as a "terms and conditions" agreement. These agreements can ensure that all conditions of submission and receipt of data electronically are known and understood by the submitting parties. This is particularly the case where terms and conditions are not spelled out in agency programmatic regulations.

c. Minimize the likelihood of repudiation.

Agencies should develop well-documented mechanisms and procedures to tie transactions to an individual in a legally binding way. For example, the integrity of even the most secure digital signature rests on the continuing confidentiality of the private key, so instituting procedures for ensuring the confidentiality of the private key would be in an agency=s interest. Similarly, in the case of electronic signatures based on the use of shared secrets like PINs or passwords, the integrity of the transaction depends on the user not disclosing the shared secret, so an agency should have procedures for encouraging the maintenance of the PIN=s integrity. If a defendant is later charged with a crime based on an electronically signed document, he or she would have every incentive to show a lack of control over (or loss of) the private key or PIN, or in the case of a PIN, that the government failed to protect the PIN on its computer system. Indeed, if that defendant plans to commit fraud, he or she may intentionally compromise the secrecy of the key or PIN, so that the government would later have a more difficult time uniquely linking him or her to the electronic transaction. Promulgating policies and procedures that ensure the integrity of security tools helps counter such fraudulent attempts.

Thus, transactions which appear to be at high risk for fraud, e.g., one-time high-value transactions with persons not previously known to an agency, may require extra safeguards or may not be appropriate for electronic transactions. One way to mitigate this risk might be to require that private keys be generated and kept on hardware tokens, making possession of the token a critical requirement. Another way to guard against fraud is to include other identifying data in the transaction that links the key or PIN to the individual, preferably something not readily available to others.

It is also important to establish that the user of the digital signature or PIN/password is fully aware of obligations he or she is agreeing to by signing at the time of signature. This can be ensured by programming appropriate ceremonial banners into the software application that alert the individual of the gravity of the action she is about to undertake. The presence of such banners can later be used to demonstrate to a court that the user was fully informed of and aware of what

he or she was signing.

d. Carefully control access to the electronic data, after receipt, yet make it available in a meaningful and timely fashion. Security measures should be in place that ensure that no one is able to alter a transaction, or substitute something in its place, once it has been received by the agency unless the alteration is a valid correction contained in an electronically certified re-transmission. This can be achieved with a digital signature because it binds the identity of the individual making the signature to the entire document, so any subsequent change would be detected. Thus, the receiving agency needs to take prudent steps to control access to the electronic transaction through such methods as limiting access to the computer database containing the transaction, and performing processing with the data using copies of the transaction rather than the original. The information may be needed for audits, disputes, or court cases many years after the transaction itself took place. Agencies should make plans for storing data and providing meaningful and timely access to it for as long as such access will be necessary.

e. Ensure the "Chain of Custody." Electronic audit trails must provide a chain of custody for the secure electronic transaction that identifies sending location, sending entity, date and time stamp of receipt, and other measures used to ensure the integrity of the document. These trails must be sufficiently complete and reliable to validate the integrity of the transaction and to prove, a) that the connection between the submitter and the receiving agency has not been tampered with, and b) how the document was controlled upon receipt.

f. Consider providing an acknowledgment of receipt. The agency's system for receiving electronic transactions may be required by statute to have a mechanism for acknowledging receipt of transactions received and acknowledging confirmation of transactions sent, with specific indication of the party with whom the agency is dealing.

g. Obtain legal counsel during the design of the system. Collection and use of electronic data may raise legal issues, particularly if it is information that bears on the legality of the process, may eventually be needed for proof in court, or involves questions of privacy, confidentiality, or liability.

Section 9. Summary of the procedures and checklist.

To summarize the process and restate the principles that agencies should employ to evaluate authentication mechanisms (electronic signatures) for electronic transactions and documents, the

following steps apply:

a. Examine the current business process that is being considered for conversion to employ electronic documents, forms or transactions, identifying customer needs and demands as well as the existing risks associated with fraud, error or misuse.

b. Identify the benefits that may accrue from the use of electronic transactions or documents.

c. Consider what risks may arise from the use of electronic transactions or documents. This evaluation should take into account the relationships of the parties, the value of the transactions or documents, and the later need for the documents.

d. Consult with counsel about any agency specific legal implications about the use of electronic transactions or documents in the particular application.

e. Evaluate how each electronic signature alternative may minimize risk compared to the costs incurred in adopting an alternative.

f. Determine whether any electronic signature alternative, in conjunction with appropriate process controls, represents a practicable trade-off between benefits on the one hand and cost and risk on the other. If so, determine, to the extent possible at the time, which signature alternative is the best one. Document this determination to allow later reevaluation.

g. Develop plans for retaining and disposing of information, ensuring that it can be made continuously available to those who will need it, for managerial control of sensitive data and accommodating changes in staffing, and for ensuring adherence to these plans.

h. Develop management strategies to provide appropriate security for physical access to electronic records.

i. Determine if regulations or policies are adequate to support electronic transactions and record keeping, or if "terms and conditions" agreements are needed for the particular application. If new regulations or policies are necessary, disseminate them as appropriate.

j. Seek continuing input of technology experts for updates on the changing state of technology and the continuing advice of legal counsel for updates on the changing state of the law in these areas.

k. Integrate these plans into the agency's strategic IT planning and regular reporting to OMB.

l. Perform periodic review and re-evaluation, as appropriate.